Inside the Digital Revolution

Heather Brooke

Technology and transparency combined to create the digital revolution, which in turn has ushered in a new form of monitory democracy. Communicative abundance and global interconnection mean the democratic franchise can expand and deepen, but the author argues that it matters who is made transparent and for what purpose. Content and context matter. Technology and transparency can be used to strengthen democracy by opening up government to citizens, but the same tools can also be used by the state to surveil and disempower citizens, thereby damaging democracy. The author uses three case studies to discuss the impact of digitizing information on power relations between citizens and states. First, her observations as the journalist and litigant in the legal case that forced the digitization of UK parliamentary expense records, which when leaked created one of the biggest political scandals in that country for decades. Second, she obtained the entire set of U.S. diplomatic cables and reported on their contents for the Guardian. *Lastly, she served as a member of the Independent Surveillance Review Panel, set up by the UK government to investigate allegations made by Edward Snowden that the UK and U.S. governments were conducting mass surveillance programs that were potentially illegal and lacked adequate oversight. The case studies show how journalism is integral not only to identifying useful civic information but also maximizing the public good from leaked information while minimizing harm.*

Heather Brooke is a professor in the department of journalism at City, University of London and she recently gained a PhD on the topic of freedom of information and the informed citizen in a democracy.

Journal of International Affairs, Winter 2016 Vol.70, No.1.

Thomas Paine described pre-Enlightenment government as "an assumption of power, for the aggrandizement of itself." By contrast the Enlightenment proposed a political system that was "a delegation of power, for the common benefit of society."[1] That promise never appeared more real than when new digital technologies combined with transparency policies to create the digital revolution. Technology enabled instant, free, and global communication and zero-cost duplication and dissemination, while transparency emerged as the antidote to corruption, injustice, abuse of power, and even inefficiency. If secrecy was not the sole cause of these societal ailments, it was seen as the necessary precondition for their existence, and "right to know" laws swept across the globe. The digitization of information enabled industrial-scale leaks and I show in this paper how a series of mega-leaks pulled back the curtain on elite structures of governance while illuminating the true costs of secrecy and how it can often hinder public accountability of public resources.

Technology and transparency were both essential in the creation of the digital revolution as they dramatically affected information flows between citizen and state, however early utopian ideas (including the author's own) that these changes inherently favored democracy were premature. Technology and transparency can be used to strengthen democracy by opening up government to citizens, but the same tools can also be used by the state to surveil and disempower citizens, thereby damaging democracy. The communications abundance of the digital revolution can democratize the public sphere by giving a platform to a wide range of voices, or it can create a climate where prejudice and propaganda run rampant. In order for technology and transparency to expand and strengthen democracy it matters *who* is made transparent and *how* technology is used. Content and context matter.

This article examines the political impact of the digital revolution using three case studies to illustrate the way digital technology and transparency combined to affect power relations between citizens and the state. After laying out a description of technology and then transparency, I will turn to the first case study: my work as the journalist and litigant in the freedom of information case that forced the digitization of UK parliamentary expense records, which when eventually published, created one of the biggest political upheavals in that country for decades. Second, I examine the leak and publication of 251,287 U.S. diplomatic

cables, which I obtained and reported on for the *Guardian*. Lastly, I discuss the revelations, by National Security Agency (NSA) contractor Edward Snowden, of mass surveillance by the UK and U.S. governments. What these case studies show is how the digital revolution is not only disrupting traditional forms of political power but challenging our very ideas about democracy. Possession and control of information allows us to demarcate who controls or influences the political system, and these battles over information are a way of testing the promise and practice of democracy to see how well citizens can access and participate in the political system. As in the case of the Members of Parliament (MPs) expenses scandal, the rhetoric of democracy was not matched in practice. Rather, the scandal revealed an elitist political system in need of substantial democratic reform.

Citizens are no longer reliant on elected officials or government institutions to represent their interests, but have a wide variety of instant and global tools at their disposal to broadcast their views. Traditional institutions and politicians are under pressure to adapt to this new democratic intensity, though the case studies show the difficulty in practicing what they preach when it comes to democracy.

Technology—The Revolution Will Be Digitized

Digitization has enabled information about government decisionmaking, policies, and outcomes to be disclosed and distributed in new formats on an unprecedented scale. There are three main revolutionary aspects of digital technology:

1. Zero-cost duplication
2. Zero-cost dissemination
3. Instant and free global communication

Digital data is expressed as a series of the digits 0 and 1. That sounds obvious but the remarkable thing about data represented in this way is its ethereality. The physical component is the server where bits of data are stored, but in its transmission to another server the data has no physical mass. Thus digital data can be shared and spread quickly and easily, just like an idea or thought. In the analog age, it cost money to share information as it meant producing another physical copy. In the digital age, the physicality has been eliminated. Now it

costs money *not* to share data. As a result, duplication and dissemination become the default and any person or organization that wants to impede this free flow of information has to spend considerable amounts of money and resources to do so. Digitization enables huge volumes of data to be compiled, stored, and analyzed quickly, at a vastly reduced cost. The ratio of data to matter on a stone tablet is poor. It gets better with paper and better still using magnetic ribbons. An exponential increase occurs with the shift to digital, which can be stored on disks, USB sticks, and microchips. Two major technological advances—in semiconductor manufacturing and fiber-optic communications—have made it possible for large volumes of information to be hosted on ever smaller physical components. An EMC-funded May 2010 report "The Digital Universe Decade – Are You Ready?" from American market research firm IDC estimated the 2010 volume of data at 1.2 million petabytes, or 1.2 zettabytes (which is 1,200 exabytes), which works out to 6.8 exabytes every two days. These are mind-boggling amounts.

This information is not static. The Internet and social networks allow it to be spread far and wide, often in real time.[2] Albert Meijer calls this phenomenon "computer-mediated transparency"' and Grimmelikhuijsen writes that it is now an "essential part of modern-day government transparency."[3] As I wrote in the introduction to *The Revolution Will be Digitised:*

> We are at an extraordinary moment in human history: never before has the possibility of true democracy been so close to realisation. As the cost of publishing and duplication has dropped to near zero, a truly free press, and a truly informed public, becomes a reality. A new Information Enlightenment is dawning where knowledge flows freely, beyond national boundaries. Technology is breaking down traditional barriers of status, class, power, wealth and geography, replacing them with an ethos of collaboration and transparency.[4]

Such an assessment now seems overly optimistic. Not only does knowledge flow freely but we have ample evidence that so, too, does ignorance, propaganda, and outright lies. Australian political and media scholar John Keane describes this as the era of "communicative abundance" and there are, as yet, no adequately ro-

bust forms of information quality control.[5] A crucial issue in the age of communicative abundance will be to find a way to balance quality control and the free flow of information while avoiding censorship and the spread of propaganda and lies. Changes in communications technology often lead to political changes.

> If assembly democracy is linked to the spoken word and representative democracy to print culture, today's democracy - what Keane calls "monitory democracy" - emerges with the rise of multimedia society.[6]

I discuss "monitory democracy" in more detail below but suffice to say, technology has often been linked with political revolutions. Karl Marx credited the railways with accelerating the ability of workers to communicate and unite: "And that union, to attain which the burghers of the Middle Ages with their miserable highways required centuries, the modern proletarians by means of railways achieve in a few years."[7] This is because informed citizens are better able to challenge hierarchies as I show in the first two case studies below. It is not an empty cliché to say that knowledge is power. The powerful know this and expend vast resources attempting to gather information and control its flow.

> Power is more than communication, and communication is more than power. But power relies on the control of communication, as counterpower depends on breaking through such control. And mass communication, the communication that potentially reaches society at large, is shaped and managed by power relationships, rooted in the business of media and the politics of the state. Communication power is at the heart of the structure and dynamics of society.[8]

The emergence of so many instant and free messaging services using text, voice, and video "has no historical precedent," and is truly revolutionary in ways that we are just beginning to understand.[9]

It is also worth noting the challenge nation-states face from the digital revolution as they seek ways to control national information and communication flow in a global, interconnected world. How does an English High Court judge enforce

contempt of court restrictions when the writer is, for example, Australian and the publication is via the American company Twitter operating under the First Amendment? One solution has been to extend national laws to the world's citizenry, as America does with the American Millennium Copyright Act, but a fairer system might be to create international norms as suggested by Dinwoodie.[10] The same is true for online crimes, which can occur on platforms with a different national jurisdiction than that of the user. There are growing cross-border publics debating global issues such as women's rights and climate change, but these online global voices have not yet found an adequate body politic.[11]

Technology and Democracy

There are two main types of democracy: "participatory" or "direct" democracy involves the direct participation of all citizens who vote on decisions that affect their lives, and "indirect" or "representative" democracy in which the people elect a representative to decide matters on their behalf.[12] There is a view that "party-centered representative democracy has now been substantially supplemented (but not replaced) with multiple forms of representing the public and holding governments accountable," writes Michael Schudson in *The Rise of the Right to Know*.[13] This new type of democracy has been given different names: "post-representative," "trans-legislative" (as a description of wider representation that is not exclusively centered on elections and legislatures), or what John Keane calls "monitory democracy."[14] Keane sees an evolution of democracy starting with the "assembly democracy" of ancient Greece to "representative democracy" of the eighteenth century, and now "monitory democracy," each prefaced by an innovation in communications technology. Monitory democracy involves "surveys, focus groups, deliberative polling, online petitions and audience and customer voting," among other things.[15] I would also add to this list journalism and right to information laws. These methods of participation and accountability are aided by the distributed communications network of the Internet and often run simultaneously parallel and outside the traditional mechanisms of party-based representation and institutional oversight. Often they are thought by citizens to be superior to formal institutional oversight, which is increasingly seen as impotent or co-opted. Aldrich wrote presciently in 2009 before the mega-leaks of WikiLeaks and Snowden, "with formalised national systems of intelligence accountability looking weaker, informal accountability

through revelations provided by a globalised media in tandem with activists and whistleblowers, may become more important."[16]

The rise of monitory democracy has not always been embraced by politicians and political institutions, including in the West as outlined in the case studies below. Not everyone likes to be scrutinized even if "in the era of monitory democracy, the constant public scrutiny of power by hosts of differently sized monitory bodies with footprints large and small makes it the most energetic, most dynamic form of democracy ever."[17] Democratic governments around the world are struggling to adapt to this potent new form of democracy.

Transparency

Supporting and enhancing the new technologies of communication and sharing are new laws and norms on transparency, specifically the Freedom of Information Act (FOIA) and other right to information (RTI) laws. If technology increased the means and methods for greater communication, then these laws provided greater content. Possession and control of information allows us to demarcate who controls or influences the political system. Freedom of information is rooted in Enlightenment values and contains a key principle of democracy; there must be access to information for all equally, or as Bavarian professor Adam Weishaupt argued in 1786, *"Aufklärung um andere wieder aufzuklären, giebt Freyheit*"—only enlightenment to enlighten others generates freedom.[18] Democracy scholar Robert Dahl lists as one of the five criteria for measuring democracy "enlightened understanding," which is the ability of citizens to be meaningfully informed about matters up for debate or decision.[19]

The increase in government openness since 1989 "is an accepted trend that commands more or less universal assent among academic analysts."[20] Transparency has become a consensual and administrative norm in public life according to many scholars.[21] Transparency is "essentially a power-reducing mechanism" so it matters *who* is made transparent. If rulers are made so, then citizens are empowered, however if citizens are made so, then they are disempowered.[22]

Openness is a modern invention according to Schudson. It is a "key element in the transformation of politics, society and culture from the late 1950s through

the 1970s."[23] Schudson gives numerous examples of how openness became a cultural phenomenon in media, popular culture, economy, and everyday life: the creation of the Securities and Exchange Commission; the publication of the Kinsey reports in 1948 and 1953 on adult sexual behavior; Daniel Ellsberg's release of the Pentagon Papers to newspapers in 1971; the Automobile Disclosure Act of 1958 requiring itemized pricing stickers on car windows, and the Automobile Safety Act and Truth in Packaging of 1966 (both spearheaded by consumer rights campaigner Ralph Nader). However, other academics view transparency as one of the oldest ideas in political thought, stemming from beliefs of intrinsic equality in existence since at least classical Greece.[24] Pericles of Athens is famous for his remarks around 430 BC in which he speaks of citizens' right to know: "Although only a few may originate a policy, we are all able to judge it."[25] Sweden was the first to enact FOI in law in 1766, but the United States is considered to have been the "traditional proponent of transparency."[26] The U.S. Freedom of Information Act, "weak as it was when passed in 1966, was a landmark development towards a more open society."[27] The Watergate scandal became a "symbolic catalyst for a new law" and in 1974 the act was amended and strengthened.[28] The importance of the U.S. law cannot be overstated. The United States had produced "a small miracle for the world" that became the model for global FOI laws.[29] It marked the beginning of what is called the "Openness Revolution" and while FOI may have begun as a means to reign in the growing state's administrative power, it soon expanded as a necessary means of ensuring other rights, most notably in the FOI campaigns of India and South Africa where secrecy bred corruption so endemic it left vulnerable citizens deprived of life's essentials such as food, water, and work.[30] In the 1990s only about a dozen countries had FOI laws. By 2006 there were 70 countries and in 2012 there were 93.[31]

Additionally, the American system of corporate disclosure was, by the 1990s, seen as the best economic model, which added to transparency's cache. While recent corporate scandals have cast doubt on the adequacy of these measures, more transparency is seen as the solution. The World Bank and IMF also adopted disclosure policies as a means to fight corruption, and the leading anticorruption organization in the world was set up in 1993 with the name Transparency International. If secrecy was the ailment, transparency was increasingly seen as a "simple solution to complex problems," with "attractive palliative qualities for

politicians and CEOs who want to be seen to be doing rather than reflecting."[32] The latest incarnation of freedom of information came with digitization and the "Open Data" movement, which has led to new collaborations between citizen and state though not always beneficial to the citizen.[33] Evgeny Morozov notes how the Hungarian cities of Budapest and Szeged provide online machine-readable transit schedules. It is government data and it is open, but few would agree this makes the Hungarian government open. In fact it is the opposite, with cuts to freedom of information and the press. We should beware of cheerleading open data as it allows "some governments to claim progress where there is none, while stalling on important reforms."[34]

Transparency and Technology as Tools for Democracy

The power of digitization to disrupt political systems is clearly seen in the MPs' expenses scandal, reaching a climax in 2009. What we witnessed in Britain was a culture clash between parliamentary officials who believed in their right to rule without public prying, confronted by a citizenry no longer content with that arrangement and newly empowered by the leak of a digitized data set of politicians' expenses.

MPs' Expenses

Although I initially trained as a journalist in the United States, the majority of my investigative journalism was conducted in the UK. I was aware of the type of documentation that underlay politicians' expense claims because I had seen similar as a reporter covering the Washington State Legislature in 1992. American journalism, both daily and investigative, is based largely on public records. This was not the case in the UK where there was no public right to access official information until implementation of the Freedom of Information Act in 2005. British journalists, I discovered, had different methods of obtaining information, some more illegitimate than others.[35]

I used Britain's new FOI law as a means of uncovering information and also to test the promise and practice of democracy. As a research tool FOI is a symbolic and political act, a form of empowerment, and I used it as such to enlighten

both myself and society. It may exist in "the humdrum world of administrative laws" but it is a "foundational element of democratic participation and accountability" and as such forms an aspect of monitory democracy.[36] From 2005 until mid-2010, I filed approximately 500 FOIs with varying levels of success. My first request to Parliament was on 2 February 2004 when I began an email correspondence with the FOI officer of Parliament.[37] I asked for MPs' expenses and she told me they would be published in October 2004. However, what came out on that date were only bulk amalgamated figures, which are useless for determining if claims are legitimate or not. So I sent my first official FOI to Parliament in January 2005 seeking the names and salaries of MPs' staff. I chose this query after interviewing a political reporter who said it was an open secret in the parliamentary lobby that MPs had family members on the payroll, some of whom did little or no work. This request was refused by Parliament. I appealed internally and then to the information commissioner who adjudicates such cases. My case came to a dead end on 4 September 2006 when the speaker of the House issued a certificate providing an absolute exemption from FOI on the grounds that the release of this information would be "likely to prejudice the effective conduct of public affairs."[38]

I moved on and asked for other types of allowances, specifically the Additional Costs Allowance (ACA), which "reimburses Members of Parliament for expenses wholly, exclusively and necessarily incurred when staying overnight away from their main UK residence…for the purpose of performing parliamentary duties."[39] At this time the ACA was £23,000 a year in addition to an MP's basic salary of £60,000. This request was also refused and I appealed to the information commissioner and then to the Information Tribunal. On 26 February 2008, after a two-day hearing in which the head of the Fees Office was questioned, the tribunal ruled in my favor that the parliamentary expense system was "deeply unsatisfactory" and the:

> laxity of and lack of clarity in the rules for ACA is redolent of a culture very different from that which exists in the commercial sphere or in most other public sector organisations today…in our judgment these features, coupled with the very limited nature of the checks, constitute a recipe for confusion, inconsistency and the risk of misuse…the shortfall both in transparency and in

> accountability is acute.[40]

The judges ordered full disclosure. However, on the last day allowable, Parliament appealed the ruling to the High Court. I defended my case and on 16 May 2008 the High Court ruled that Parliament had to disclose the information.[41] The expenses of the 14 MPs in the test case were published, but the ruling committed Parliament to publishing the records for *all* 646 MPs. A deadline was set for October 2008, but the date came and went, as did another deadline of December. The scale of the publication was set out in the following parliamentary answer by Nick Harvey to a question about the digitization process:

> It is therefore planned that the scanning of some 1.3 million documents and first stage redaction to remove details such as addresses, telephone numbers, banking details and account numbers will be undertaken under secure conditions by a contractor familiar with providing services to Government and Parliament whose staff have been security cleared.[42]

On 15 January 2009, leader of the House Harriet Harman announced that motions would be brought forward on 22 January to exempt Parliament from the FOIA. That would mean no expenses published—ever. There was public uproar and the proposal quickly capsized under the weight of all the negative publicity. Still there was no indication of when Parliament would publish the information. Eventually the entire unredacted digitized dataset was copied onto a hard drive and leaked. John Wick, the middleman who brokered the deals between an unknown parliamentary insider and various newspapers, explained the source's motivation for the leak:

> critical information—particularly the removal of addresses from the files—would lead to many of the scams never being publicly exposed. The source was adamant that the key thing was that both the information and the way in which it was handled should be in the public domain and that its release was in the public interest.[43]

A few newspapers picked one or two items from the data, but it wasn't until the

Daily Telegraph paid £110,000 for the entire dataset, and proceeded to roll out weeks of stories from its investigations, that the scandal reached critical mass. Media and public attention focused on high-profile and unusual claims such as a duck house and Douglas Hogg's moat cleaning, however there were many more serious abuses such as fraud for which five MPs and two lords were imprisoned. A formal audit of the expenses system reported that it was "deeply flawed" and a total of 389 MPs were ordered to return some £1.3milion.[44]

How did this advance the digital revolution? Crucial to the leak was the fact that without FOI and the subsequent court battle, the data would not have been digitized. If not digitized there would have been no disk to leak. "Only the total claimed by each MP is kept in electronic format," the Commons' FOI officer Bob Castle had stated in a letter to the information commissioner. If not leaked, Parliament would have been able to secretly expand and reinterpret the narrow exemption for sensitive personal information. Indeed, the official version eventually published in June 2009 excised all the worst abuses.[45]

As it was, the leak of the unredacted digital dataset prevented Parliament from interpreting and censoring the data and instead reporters and citizens viewed it raw. The resulting exposés "destabilized the government," and led to a wave of resignations (the speaker plus six ministers) and nearly a fifth of MPs (120) stepped down at the 2010 election.[46] In the first days of publication, parliamentarians called on the metropolitan police to open a criminal investigation into the *Daily Telegraph* for possession of stolen property, but this went nowhere due in large part to the weight of public opinion against MPs.[47] A British election study from June 2009 showed 95 percent of the public aware of the scandal, 91 percent very angry about it, and 82 percent saying MPs who abused the system should resign immediately.

The scandal has been described in superlative terms both for its journalistic and political impact. It was "one of the biggest stories in modern British history," one that "rocked cultural, political and journalistic spheres."[48] Politically, it was an "incendiary device thrown directly at the political establishment," and produced a scandal that "shook Westminster to the core."[49] It led to reforms of the MP allowances system and, with the Parliamentary Standards Act of 2009, the establishment of the Independent Standards Authority. According to Worthy

and Hazell et al., the scandal also led to "intense discussion of constitutional reform" with Gordon Brown and David Cameron vying in the general election of 2010 over who could offer the most reform.[50] Cameron's platform included public recall power of MPs, which became the Recall of MPs Act 2015. A new government was elected in May 2010 on a mandate of transparency and the UK went from being an open data backwater to ambitious world leader.[51] The (London) *Times* summed up the changes with a front-page article headlined "New order":

> Parliament was forced to surrender its ancient right to run its own affairs on a momentous day in which the Speaker, Michael Martin, paid for the scandal over MPs' expenses with his job. The Prime Minister announced that the financial affairs of MPs would be taken over by independent regulators.[52]

However, the reforms were not nearly radical enough. Importantly, expense information was still not directly accessible to the public, but rather mediated by a newly created bureaucracy. Perhaps as a result, the media exposed a steady stream of MPs abusing public expenses, and Parliament's reputation worsened. A 2012 YouGov poll found just 26 percent of people thought most MPs were honest, down from 34 percent in 2010. Only 13 percent thought most MPs were in touch with the daily lives of their constituents in 2012 and the proportion of people believing MPs were principled was down six points to 26 percent. The majority of people, 72 percent, agreed with the view that "not enough had been done to stop MPs wrongfully claiming expenses and MPs are probably getting up to the same abuses as before," compared to 13 percent who thought Parliament had learned from the scandal and new MPs would behave better.[53]

WikiLeaks

Freedom of information exists on a continuum with mega-leaks at the far end and it was only a matter of time, I thought, before other political systems were hit by digitized mega-leaks similar to the MPs' expense scandal. I started research on my next book *The Revolution will be Digitised* and came across WikiLeaks founder Julian Assange in March 2010 at a Norwegian investigative journalism conference.[54] During lunch, he told me about secret footage he'd ob-

tained that showed "collateral murder by a major Western government," which he later said was the United States. This was the "Collateral Murder" video.[55] At that time, I was impressed with WikiLeaks because their publication of previously secret information indicated a willingness and boldness to push the limits of transparency. However, I came to the conclusion that Assange was an inconsistent and unreliable source, and his actions, as I witnessed them, ran counter to his professed ideologies. I focused my reporting elsewhere and it was through another WikiLeaks volunteer that I was leaked a copy of the entire unredacted dataset of the U.S. diplomatic cables, described at the time as "the largest set of confidential documents ever to be released into the public domain."[56] Initially, I tried analyzing the dataset myself but at a quarter of a million records, it was too vast. Also, the material was of a sensitive nature, and as such I needed legal, editorial, and institutional support. I therefore partnered with the *Guardian* and we worked on a months-long investigation culminating in a series of articles from 28 November 2010 to January 2011. The data set was also shared with the *New York Times* who ran a parallel set of stories.

Leaks are often committed with the hope of "destabilizing the epistemic space."[57] They create an existential challenge for the secret state but can be restorative for democracy. They can highlight the doublethink of states when rhetoric of openness and access to information is applied directly.[58] This was clearly seen when, in January 2010, secretary of state Hillary Clinton gave a speech devoted to Internet freedom:

> On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single Internet where all of humanity has equal access to knowledge and ideas.[59]

She described a new kind of "information curtain" that was descending across much of the world where countries erected electronic barriers to stop their citizens accessing portions of world networks. She urged private companies to stand up to foreign governments who sought to control the Internet and promised that the U.S. government would support technology designers to circumvent blocks or firewalls. However, when it was the U.S. government's information that was duplicated and disseminated, there was an entirely different response.

U.S. officials announced an investigation into WikiLeaks and Clinton said the government would take "aggressive steps" to hold responsible those who "stole" the data.[60] U.S. Army intelligence analyst Chelsea Manning (at the time Pfc. Manning went by Bradley Manning) was arrested in connection with the leak on 27 May 2010 and transferred to the Marine Corps Base in Quantico, Virginia on 29 July 2010. The soldier's ill treatment at the facility was described by State Department spokesman Philip Crowley as "ridiculous and counterproductive and stupid."[61] This candor prompted Crowley's resignation two days later, while Manning was transferred to a medium-security jail in Fort Leavenworth, Kansas. The soldier was convicted by a military judge in July 2013 of 17 of 22 charges, including violations of the Espionage Act, for copying and disseminating classified military field reports, State Department cables, and assessments of detainees held at Guantanamo Bay, Cuba. However, she was acquitted of the most serious charge, aiding the enemy. In August 2013 Manning was sentenced to thirty-five years in prison with the possibility of parole after eight years. During the trial Manning read from a 35-page statement, saying she leaked the cables "to show the true cost of war."[62]

In this case the leaker was not protected by public opinion. A Pew Research Center study in December 2010 found that 60 percent of those aware of the diplomatic cables story believed leaking State Department cables harmed public interests. And 31 percent thought it was in the public interest. Interestingly, the public made a distinction between WikiLeaks itself and the press handling of the data, with 39 percent saying the media had struck the right balance reporting on the leaks and 14 percent saying they held back too much.

The publication of the U.S. diplomatic cables marked a definitive shift toward what some called "radical transparency" and others called "massive, vigilante disclosure."[63] Some credited the cable publication with the Tunisian uprising in January 2011, an event which led to the Arab Spring.[64] An article in *Foreign Policy*, "The First Wikileaks Revolution?" claimed that site disclosures "acted as a catalyst: both a trigger and a tool for political outcry."[65] However, WikiLeaks itself did little reporting on the data. That was the job of the journalists. And it was the source who provided the information and who faced the consequences. Some have conflated Assange's subsequent arrest in December 2010 with the publication of the diplomatic cables, when in fact it was the result of sexual

assault and rape allegations made by two women in Sweden.

In time, the hype about this novel leaking site was replaced with a more tempered view: "Wikileaks only created the illusion of a new era in transparency" said Roberts, and early advocates had "overstated the scale and significance of the leaks."[66] WikiLeaks role in of itself has been consistently overstated, however the leaked information and subsequent articles allowed for a greater understanding about the reality of politics, diplomacy, and corruption. For this reason, an argument can be made that the leaks had an immediate impact on the Arab Spring protests, in Tunisia especially, because it gave people an unvarnished view of their rulers as real, fallible human beings. Amnesty International's secretary general, Salil Shetty, has said that:

> The year 2010 may well be remembered as a watershed year when activists and journalists used new technology to speak truth to power and, in so doing, pushed for greater respect for human rights.[67]

So much of elite political systems depend on an illusion of infallibility and superiority. Among the revelations reported in the *Guardian* were many instances where elites were shown to be fallible humans acting in ways childish, immoral, or corrupt.[68] The cables also revealed numerous examples across the world where an elite few were privately benefiting from public resources.[69] I believe these revelations illuminated the costs of secrecy, and how it had aided elite structures of governance while hindering public accountability of public resources. The publication also challenged authoritarian views that tend to maximize the risks of disclosure while minimizing those of secrecy. Officials claimed publication would result in "untold incalculable damage to the nation's military personnel, national security, and diplomatic efforts," however as no clear evidence emerged of significant damage they had to retreat from this position.[70] Perhaps as a result, courts may be more skeptical in the future of claims of the catastrophic consequences of disclosure.

In these two case studies, we can see that digitization was a means to shake the pillars of elite rule, not just in the UK but the United States, Middle East, and around the world. How successful these attempts have been is very much open

to debate. What is certain is that political elites felt increasingly challenged and, where public opinion was on their side, fought back using state institutions. In some instances, such as the Arab Spring, the successful challenge of autocratic regimes did not lead to the promised expanding of the democratic franchise. Rather it resulted in a shift to a different group of elites operating in a similarly autocratic tradition.[71]

Transparency and Technology as Tools of Oppression

Technology has the ability to magnify power, but rates of adoption vary. Small groups and individuals can adapt faster to new technology than large institutions, and so for a time technology empowered small groups and individuals in relation to the state as in the two cases presented above. Security engineer Bruce Schneier estimates that it took about a decade for traditional power to adapt to new technologies, but once they did, their powers were magnified exponentially.[72] Tom Steinberg, the creator and founder of UK civic technology organization My Society, writes in an essay:

> few people are less happy these days than privacy campaigners. The fact that everyone carries sensor laden mobile phones makes national security agencies more powerful than they were before. Even where privacy protecting technologies exist, they cannot be said to be equal and opposite in effect to the ubiquitous computing we now live amongst. Mobile computing is a permanently power shifting technology that permanently empowers the security services.[73]

Technology now exists that enables companies and governments to monitor our conversations, commercial transactions, and movements, and to make predictive decisions about us based on this data. Not only are there more technologies to surveil citizens, but also more entities that want to do so. The Internet business model has become one based on surveillance.[74] It used to cost states money and resources to spy on its citizens, but now thanks to technology, we have a variety and scope of surveillance that is "unprecedented in human history."[75] This was made clear in June 2013 when the *Guardian* and *Washington Post* began publishing a series of articles based on revelations from Edward Snowden, a former

systems administrator of the National Security Agency.

Snowden Revelations

Before Snowden, little attention was given to the rise of state surveillance and official secrecy that followed terrorist attacks on 11 September 2001, particularly related to intelligence agencies. The UK's first information commissioner, Richard Thomas, warned the country was "sleepwalk[ing] into a surveillance society," and American journalist Ted Gup criticized the media for failing to report what has been "one of the more significant stories of our lifetime - an emerging 'secretocracy' that threatens to transform American society and democratic institutions."[76] A large part of the problem for journalists, including myself, was the dearth of information. In the UK, intelligence agencies are exempt from FOIA and in the United States several scholars have noted the rise in official secrecy after the 11 September 2001 attacks.[77] There are very few legitimate ways to access the information needed for verification and to meaningfully report on security services. The rise in outsourcing and privatization further erodes access.[78] Added to this has been the dramatic rise in the prosecution of whistleblowers and journalists by the U.S. government.[79]

Despite, or perhaps because of, this rise in official secrecy, Snowden went to journalists Laura Poitras and Glenn Greenwald with information obtained while working as a contractor for the National Security Agency. The revelations began with an article describing how the NSA was accessing phone records of millions of U.S. Verizon customers using a secret bulk warrant.[80] A day later top secret documents were published alleging the NSA had obtained direct access to the systems of Google, Facebook, Apple, and other U.S. Internet companies in a program called Prism, though these companies denied the existence of backdoors.[81] Another article disclosed that the NSA's British equivalent, the Government Communications Headquarters (GCHQ), also had access to Prism and additionally was tapping fiber optic cables to intercept data flowing through the global Internet in a program called Tempora.[82] Other revelations included NSA surveillance of world leaders hacking operations, intercepting phone data, and "nearly everything a user does on the internet."[83]

Public opinion to the leaks was mixed with 45 percent saying it served the

public interest while 43 percent thought it had harmed it. A majority, 56 percent, thought a criminal case should be made against Snowden, with 32 percent opposed.[84] The U.S. government charged Snowden with theft of government property, and two charges under the 1917 Espionage Act, which together would incur a maximum sentence of thirty years in prison. The Espionage Act does not allow for public interest or whistleblower defense. Additionally, the United States submitted extradition requests to numerous countries. Snowden eventually sought asylum in Russia.

As a result of the Snowden disclosures, public awareness about online privacy and government surveillance grew, and a number of specialist reporters now cover security services. There is even a well-funded organization devoted to this coverage, the Intercept, employing some of the journalists who worked with Snowden. Technology companies began building encryption into their products, and on 2 June 2015, the USA Freedom Act became law, ending the bulk collection of phone call metadata directly by the NSA. However, phone companies still had to retain it, only now the government would have to get approval from the Foreign Intelligence Surveillance Court. In the UK, three reviews were undertaken on security services and surveillance. I sat on one, the Independent Surveillance Review Panel, and from June 2014 until the publication of our report 14 July 2015 we met, took evidence, and had site visits to assist our investigation.[85] In my view, our report did not place enough emphasis on the harm resulting from mass, or bulk, surveillance and I did not agree with the statement "we have seen no evidence that the British Government knowingly acts illegally in intercepting private communications."[86] That is only because we were unable to see enough evidence to make a judgment either way. This is the difficulty of holding the secret state to account. Claims and evidence cannot be verified or tested.

Security services are adamant that digital technology and communications have led to a large and expanding number of threats, not just with international terrorism but industrial, military, and state espionage, organized criminality, and child sexual exploitation. Theresa May, as home secretary, put it bluntly while arguing for unprecedented spying powers on citizens online: "this is quite simply a question of life and death, a matter of national security. We must keep on making the case until we get the changes we need."[87] Bulk and mass surveillance

has been the state's answer to the problem of digital technology and online criminality and the disclosures by Edward Snowden reveal that intelligence agencies did not wait for a democratic mandate to set up these surveillance systems. As a result, there were concerns that they were operating outside the law.

In the UK, the government's ultimate response to Snowden has been to introduce the Investigatory Power Bill, which would legitimize the current practices of mass or "bulk" surveillance.[88] The French government passed a sweeping surveillance law in May 2015.[89] In 2016, Japan's Supreme Court upheld the government's blanket surveillance of the country's Muslim community.[90]

These are worrying signs for the future of democracy, as a society that permits "the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy."[91] Richards identifies two main harms resulting from surveillance: it chills human thought and it leads to abuse of power.[92] Psychological studies have shown that people resort to more conformist and compliant behaviors when they think they are under surveillance.[93] Two recent studies have provided empirical evidence of the "chilling effect" of surveillance. Elizabeth Stoycheff found that a majority of participants, when made aware of government surveillance, were significantly less likely to speak out in hostile opinion climates.[94] Jonathon Penney found a large, statistically significant, and immediate drop in total views for privacy-sensitive Wikipedia articles after June 2013 (the publication date of the Snowden articles), and that the drop was long term.[95] If people are deterred from informing themselves or researching controversial subjects, they will inevitably be less informed and "our broader processes of democratic deliberation will be weakened."[96]

Conclusion

Technology can be used to strengthen democratic values and processes or to damage them. Certainly, digitized information is harder to control, as seen in all three case studies. However, it is perfectly possible to bend technology to suit the needs of bureaucracies and power, which was made clear via the Snowden revelations. "Without a conscious and deliberate effort to use the new technology of telecommunications in behalf of democracy, it may well be used in ways harmful to democracy."[97] It matters *who* is made transparent—the citizen or the

state. More than at any other time in history, the state can match its desire to know "with the means to collect, monitor, and (even) predict the behaviors of their subjects/citizens."[98] Whether or not this makes "us" safer depends on who this "us" refers to and how we define safety and freedom.

It also matters *what* is made transparent and the context of publication. Transparency when combined with technology has created leaks on an industrial scale. Such mega-leaks allow the public to pull back the curtain on elite structures of government. What they find may not be pretty, nor able to withstand public scrutiny. The case studies show how journalism is integral not only to identifying useful civic information, as evidenced in MPs' expenses, but also maximizing the public good from leaked information while minimizing harm. Data dumps are not capable of this nuance. In the three case studies put forward, content and context materially affected public opinion of the leaks. People were more in favor of mediated leaks than data dumps, and more in favor of information about how public officials spend public money than national security or defense. Sanctions against the leaker/publisher lessened when public opinion viewed the leaked material as strongly in the public interest.

Transparency and technology have led to a digital revolution, which in turn has ushered in a new form of monitory democracy. Communicative abundance and global interconnection mean the democratic franchise can expand and deepen. As technology creates new ways for citizens to have their rights and interests heard and represented in the community, this has led to a "clash between twenty-first century expectations, technologies and transparency challenging a nineteenth-century model of democracy and participation."[99] Our democratic institutions need to wake up to this new reality and radically reform in line with increased expectations of citizen equality. If they fail, they risk eroding public confidence and democratic institutions may no longer be seen as serving the public interest but the private interests of an elite few.

Endnotes

1 Thomas Paine, *Rights of Man*, Eric Foner, ed. (New York, NY: Penguin, 1790 (reprinted 1985)).
2 S. Grimmelikhuijsen, Transparency & trust: An experimental study of online disclosure and trust in government (PhD dissertation, Utrecht School of Governance, 2012); S. Grimmelikhuijsen, "Linking transparency, knowledge and citizen trust in government: An experiment," *International Review of Administrative Sciences* 78, no. 1 (2012), 50-73; S. Grimmelikhuijsen, "Being transparent or spinning the message? An experiment into the effects of varying message content on trust in government," *Information Polity* (2011), 35-50.
3 A.J. Meijer, "Understanding modern transparency," *International Review of Administrative Sciences* 75, no.2 (2009), 255-269; S. Grimmelikhuijsen, G. Porumbescu, B.Hong, and T. Im, "The effect of transparency on trust in government: A cross-national comparative experiment," *Public Administration Review* 73, no.4 (2013), 575.
4 Heather Brooke, *The Revolution Will be Digitised* (London: Windmill Books, 2011 (reprinted 2012)).
5 John Keane, "Democracy in the age of Google, Facebook and WikiLeaks" (article, University of Melbourne, 18 May 2011).
6 Michael Schudson, *The Rise of the Right to Know* (Cambridge, MA: The Belknap Press of Harvard University Press, 2015), 234.
7 Karl Marx and Friedrich Engels, *The Communist Manifesto,* L.M. Findlay, ed. and tran. (Toronto: Broadview, 1848 (repringted 2004)), 70.
8 M. Castells, *Communications Power* (Oxford: Oxford University Press, 2013), 3.
9 Keane, "Democracy in the age of Google, Facebook and WikiLeaks," 3.
10 Graeme Dinwoodie, "A New Copyright Order: Why National Courts Should Create Global Norms," *University of Pennsylvania Law Review* 149, no. 2 (December 2000), 469-580.
11 Keane, "Democracy in the age of Google, Facebook and WikiLeaks."
12 John Keane, *The Life and Death of Democracy* (New York: Simon & Schuster, 2009).
13 Schudson, *The Rise of the Right to Know*, 230.
14 John Keane, "Monitory Democracy" (paper, ESRC Seminar Series "Emergent Publics," Open University, 13-14 March 2008).
15 Ibid., 10.
16 Richard Aldrich, "Regulation by revelation? Intelligence, the media and transparency," in *Spinning Intelligence,* Robert Dover and Michael Goodman, eds. (New York, NY: Columbia University Press, 2009), 10.
17 John Keane, *The Life and Death of Democracy*, 743.
18 J. Israel, *A Revolution of the Mind: Radical Enlightenment and the Intellectual Origins of Modern Democracy (*Princeton; Oxford: Princeton University Press, 2009), 85, citing Adam Weishaupt, *Apologie der Illuminaten* (Frankfurt and Leipzig, 1786), 46.
19 R.A. Dahl, *Democracy and its critics* (London; New Haven: Yale University Press, 1989), 122.
20 Aldrich, "Regulation by revelation? Intelligence, the media and transparency," 15.
21 Schudson, *The Rise of the Right to Know*; M. Fenster, "Transparency in search of a theory," *European Journal of Social Theory* 18, no. 2 (2015), 150–167; A.J. Meijer, "Introduction to the special issue on government transparency," *International Review of Administrative Sciences* 78, no. 1 (2012), 3-9; C. Hood, "Transparency in Historical Perspective," in *Transparency: The key to better governance?* C. Hood and D. Heald, eds. (Oxford: Oxford University Press, 2006), 3-23.
22 Grimmelikhuijsen et al., "The effect of transparency on trust in government: A cross-national comparative experiment," 583.
23 Schudson, *The Rise of the Right to Know*, 5.

24 Hood, "Transparency in Historical Perspective;" Dahl, *Democracy and its critics.*
25 Thucydides, *History of the Peloponnesian War* II, 37-41.
26 A. Florini, "Introduction: The battle over transparency," in *The right to know: transparency for an open world*, A Florini, ed. (New York, NY: Columbia University Press, 2007), 9.
27 Schudson, *The Rise of the Right to Know*, 30.
28 B. Worthy, "Freedom of Information and the MPs' Expenses Scandal," in *At the Public's Expense? The Political Consequences of the 2009 British MPs' Expenses Scandal*, J. Vanheerde-Hudson, ed. (London: Palgrave, 2014), 27-43.
29 Schudson, *The Rise of the Right to Know*, 62.
30 Schudson, *The Rise of the Right to Know*; Florini, "Introduction: The battle over transparency."
31 Toby Mendel, "Freedom of Information: A Comparative Legal Survey, Second Edition" (report, UNESCO, 2008); Roger Vleugels, "Overview of All 90 FOIA Countries & Territories," (fringe special, September 2009); Florini, "Introduction: The battle over transparency."
32 C. Birchall, "Radical Transparency?" *Cultural Studies: Critical Methodologies* 14, no. 1 (2014), 77.
33 D. Lathrop, and L. Ruma, eds., *Open Government: Collaboration, Transparency, and Participation in Practice* (Cambridge: O'Reilly, 2010).
34 Evgeny Morozov, *To Save Everything, Click Here* (New York, NY: Public Affairs, 2013), 96.
35 *For an extensive look at the inner workings of British journalism see* Nick Davies, *Hack Attack* (London: Chatto & Windus, 2014) and Nick Davies, *Flat Earth News* (London: Chatto & Windus, 2008).
36 Fenster, "Transparency in search of a theory."
37 *A detailed account of this case is in* Heather Brooke, *The Silent State* (London: Windmill Books, 2010 (reprinted 2011)), chapter 8.
38 *The certificate is referred to in Information Commissioner Decision Notice FS50073128: Heather Brooke vs House of Commons.*
39 House of Commons Department of Finance and Administration, "The Green Book: Parliamentary Salaries, Allowances and Pensions" (2006), 294.
40 Information Tribunal EA/2007/0060 and others, 26 February 2008.
41 High Court, EWHC 1084 (Admin) Case No: CO2888/2008, 2008.
42 High Court, Deb 1, July 2008, c741W.
43 J. Wick, "Whistleblower John Wick: I am proud to have exposed MPs' expenses scandal," *Daily Telegraph*, 22 May 2009.
44 Chris Tryhorn, "Telegraph paid £110,000 for MPs' expenses data," *Guardian*, 25 September 2009; House of Commons Members Estimate Committee, "Review of Past ACA Payments" (London: The Stationary Office Limited, 2010); See also A. Eggers and A. Fischer, "Electoral Accountability and the UK Parliamentary Expenses Scandal: Did Voters Punish Corrupt MPs?" (working paper, LSE Department of Government, 2011).
45 Robert Winnet and James Kirkup, "Blackout: the great MPs' expenses cover-up," *Daily Telegraph,* 18 June 2009.
46 B. Worthy, "More Open but Not More Trusted? The Effect of the Freedom of Information Act 2000 on the United Kingdom Central Government," *Governance* 23, no. 4 (2010), 562.
47 "MPs' expenses: Commons authorities ask police to investigate leak," *Daily Telegraph,* 8 May 2009.
48 Matt Burgess, *Freedom of information: a practical guide for UK journalists* (London: Routledge, Taylor & Francis Group, 2015), 138.
49 A. Kelso, "Parliament on its knees", *Political Quarterly* 80 (2009), 334; J. VanHeerde-Hudson, *The political costs of the 2009 British MPs' expenses scandal (*Basingstoke: Palgrave Macmillan, 2014).
50 R. Hazell, B. Worthy, and M. Glover, *The impact of the freedom of information act on central government in the UK (*Basingstoke: Palgrave Macmillan, 2010).
51 G. Moss and S. Coleman, "Deliberative Manoeuvres in the Digital Darkness: e-Democracy

Policy in the UK," *British Journal of Politics & International Relations* 16, no. 3 (2014), 410-427.

52 Philip Webster, "New order," *Times*, 20 May 2009.

53 Anthony Wells, "MPs expenses, again," YouGov, 23 October 2012.

54 Heather Brooke, *The Revolution Will be Digitised* (London: Windmill Books, 2011 (reprinted 2012)).

55 WikiLeaks, 5 April 2010, https://collateralmurder.wikileaks.org.

56 WikiLeaks, "Cablegate: 250,000 US Embassy Diplomatic Cables," 2011, https://wikileaks.org/cablegate.html.

57 L. Quill, *Secrets and Democracy: From Arcana Imperii to Wikileaks* (Palgrave MacMillan, 2014), 84.

58 On the ecosystem of leaks see, for example, David Pozen, "The leaky leviathan: Why the government condemns and condones unauthorized disclosures of information," *Harvard Law Review* 127 (2013) and Sissela Bok, *Secrets: On the ethics of concealment and revelation* (Vintage, 1989).

59 Hillary Clinton, "Remarks on Internet Freedom" (speech, Newseum, Washington DC: 21 January 2010).

60 Ewen MacAskill, "Hillary Clinton attacks release of US embassy cables," *Guardian,* 29 November 2010.

61 Matt DeLong, "P.J. Crowley resigns after Bradley Manning comments," *Washington Post*, 13 March 2011.

62 Alexa O'Brien, "Bradley Manning's full statement," *Salon*, 1 March 2013.

63 Micah Sifry, *Wikileaks and the Age of Transparency* (Berkeley, CA: Counterpoint Press, 2011); M. Fenster, "Disclosure's effects: WikiLeaks and transparency," *Iowa Law Review* 97, no. 3 (2012), 753.

64 *The publication of the following cable in particular was credited with radicalising an already angry and disenfranchised Tunisian population. WikiLeaks, "Cable o8TUNIS6yç, Corruption in Tunisia: What's Yours Is Mine," 2012.*

65 E. Dickinson, "The First Wikileaks Revolution?" *Foreign Policy*, 13 January 2011.

66 A. Roberts, "Wikileaks: The illusion of transparency," *International Review of Administrative Sciences* 78 (2012), 117.

67 Peter Walker, "Amnesty International hails WikiLeaks and Guardian as Arab spring 'catalysts,'" *Guardian*, 13 May 2011.

68 See for example Heather Brooke, David Leigh, and Rob Evans, "WikiLeaks cables: 'Rude' Prince Andrew shocks US ambassador," *Guardian*, 29 November 2010; Heather Brooke, "WikiLeaks cables: Vatican refused to engage with child sex abuse inquiry," *Guardian*, 11 December 2010; Heather Brooke, "WikiLeaks cables: Saudi princes throw parties boasting drink, drugs and sex," *Guardian*, 7 December 2010.

69 An entire list of articles related to the U.S. embassy cables can be found on the *Guardian* website: http://www.theguardian.com/us-news/the-us-embassy-cables. As of 6 March 2016 there were 1,491 articles listed.

70 Fenster, "Disclosure's effects: WikiLeaks and transparency," 806.

71 Morozov, *To Save Everything, Click Here*; A. Taylor, *The people's platform: taking back power and culture in the digital age* (London: Fourth Estate, 2014).

72 Bruce Schneier, "The future of Internet, Privacy & Security" (remarks, Tedx, Cambridge: October 2013).

73 Tom Steinberg, "The Pill versus the Bomb: What Digital Technologists Need to Know About Power," *Medium,* 2015.

74 Neil Richards, "The Dangers of Surveillance," *Harvard Law Review* (25 March 2013), 1936.

75 Ibid.

76 Jenny Booth, "UK 'sleepwalking into a Stasi state,'" *Guardian*, 16 August 2004; Ted Gup, "Investigative Reporting About Secrecy," *Nieman Reports*, 15 March 2008.

77 Aldrich, "Regulation by revelation? Intelligence, the media and transparency;" Alasdair Rob-

erts, *Blacked Out: Government Secrecy in the Information Age* (New York, NY: Cambridge University Press, 2006).

78 Dana Priest and William M. Arkin, "National Security Inc." *Washington Post*, 20 July 2010.

79 Aldrich, "Regulation by revelation? Intelligence, the media and transparency,"29-30; David Pozen, "The leaky leviathan: Why the government condemns and condones unauthorized disclosures of information," *Harvard Law Review* 127 (2013), 512-635.

80 Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *Guardian*, 6 June 2013.

81 Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *Guardian*, 7 June 2013.

82 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, 21 June 2013.

83 Laura Poitras, M. Rosenbach, and H. Stark, "'A' for Angela: GCHQ and NSA targeted private German companies and Merkel," *Der Spiegel*, 29 March 2014; Der Spiegel Staff, "Inside TAO: Documents reveal top NSA Hacking unit," *Der Spiegel*, 29 December 2013; James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep,"' *Guardian*, 16 January 2014; Glenn Greenwald, "XKeyscore:NSA tool collects 'nearly everything a user does on the internet,"' *Guardian*, 31 July 2013.

84 "Obama's NSA Speech Has Little Impact on Skeptical Public" (report, Pew Research Center, 20 January 2014).

85 *A full list of our site visits and evidence sessions can be found in the appendix of the report "A Democratic Licence to Operate."*

86 "A Democratic Licence to Operate: Report of the Independent Surveillance Review" (report, Royal United Services Institute for Defence and Security Studies, July 2015).

87 *Theresa May: There is no surveillance state," BBC, 24 June 2014.*

88 *For current status of this bill see http://services.parliament.uk/bills/2015-16/investigatorypowers.html.*

89 "French parliament approves new surveillance rules," BBC, 6 May 2015.

90 M. Payton, "Japan's top court has approved blanket surveillance of the country's Muslims," *Independent*, 29 June 2016.

91 J.E. Cohen, "What privacy is for," *Harvard Law Review* 126, no. 7 (2013), 1912.

92 Richards, "The Dangers of Surveillance."

93 Ibid.

94 Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* (2016), 1-16.

95 Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" *Berkeley Technology Law Journal*, (2016).

96 Ibid., 51.

97 Dahl, *Democracy and its critics*, 339.

98 Quill, *Secrets and Democracy: From Arcana Imperii to* Wikileaks, 10.

99 David Richards and Martin Smith, "In Defence of British Politics Against the British Political Tradition," *Political Quarterly* 86, no. 1 (January–March 2015), 46.